Estudio y Análisis de estrategias de seguridad para Cloud Computing híbridos

Nelson Rodríguez[1], Adriana Valenzuela[2], María Murazzo[3], Susana Chávez[4], Adriana Martín[5], Daniela Villafañe[6]

Departamento e Instituto de Informática - F.C.E.F. y N. - U.N.S.J.

Complejo Islas Malvinas. Cereceto y Meglioli. 5400. Rivadavia. San Juan

[1]nelson@iinfo.unsj.edu.ar [2]franciscaadriana.valenzuela@gmail.com [3]marite@unsj-cuim.edu.ar

[4]schavez@iinfo.unsj.edu.ar [5]arianamartinsj@gmail.com [6]villafane.unsj@hotmail.com

Resumen

Cloud Computing (2C) es un modelo de computación y de negocios que ha transformado los modos de cómo las empresas utilizan y adquieren los recursos de Information Technology (IT). Entrega mayor eficiencia, escalabilidad masiva y más rápido y fácil desarrollo de software. Inicialmente las empresas accedieron a Cloud Públicos, pero luego comenzaron a montar sistemas híbridos que ofrecen las ventajas de Cloud Computing sumado a la privacidad de los datos que consideren estratégicos. Así, los datos estratégicos están almacenados en servidores privados y muchos otros como sitios Web y servicios de e-mail se encuentran en algún proveedor remoto. Una solución híbrida permite la integración de ambos sistemas. Garantizar la seguridad de los datos no resulta sencillo, dado que hay que integrar el modelo de seguridad del Cloud público con el privado, pero a su vez no dejar ningún punto de vulnerabilidad y permitir que esta integración se realice de forma adecuada. Por lo tanto la línea de investigación plantea un análisis profundo de todas las estrategias de seguridad en ambos Clouds y la forma en que van a interactuar ambas manteniendo los parámetros de privacidad, integridad, confidencialidad, autenticidad y disponibilidad en los niveles que exigen los negocios actualmente.

Palabras clave: *Hybrid Cloud Computing, Cloud Security, IaaS, SaaS, PaaS*

Contexto

El presente trabajo se encuadra dentro del área de I/D Seguridad Informàtica y se enmarca dentro del proyecto de investigación: Cloud Computing con herramientas libres para evaluación de modelos de despliegue híbrido, iniciado en enero de 2014, con una duración de dos años y que tiene como unidades ejecutoras al Departamento e Instituto de Informática de la FCEFyN de la UNSJ. El grupo de investigación viene realizando varios proyectos relacionados de hace más de 15 años con numerosas publicaciones y formación de recursos humanos en el área.

Introducción

2C es un modelo que proporciona nuevos beneficios a usuarios, compañías e instituciones. Es una macroestructura distribuida que computa con mínimo esfuerzo y costos en recursos de informática, altamente disponibles y con dinamismo escalable [1].

En los últimos años se pasó de un modelo centralizado, a un modelo ampliamente distribuido en donde conviven data centers, computadoras personales,

clusters y dispositivos móviles de los más variados [2],

Las formas tradicionales en que las empresas utilizan y adquieren los recursos tecnológicos han evolucionado con el auge de 2C, ofreciendo mayor eficiencia, escalabilidad masiva y más rápido y fácil desarrollo de software [3].

Representa un modelo de prestación de servicios de negocio y tecnología que permite acceder a un catálogo de servicios estandarizados y responder a las necesidades del negocio de forma flexible y adaptativa, en caso de demandas no previsibles o de picos de trabajo, pagando únicamente por el consumo efectuado. Es el resultado de la evolución de varias tecnologías tales como utility computing, computación bajo demanda, computación elástica y grid computing [4].

En este modelo los recursos y servicios informáticos, tales como infraestructura, plataforma y aplicaciones, son ofrecidos y consumidos como servicios a través de Internet sin que los usuarios tengan que tener ningún conocimiento de lo que sucede detrás [5].

Se divide a 2C en las siguientes capas: Software como Servicio (SaaS), Plataforma como Servicio (PaaS) e Infraestructura como Servicio (IaaS) [6], aunque se han sugerido otras capas como Hardware como Servicio (HaaS) y Database como Servicio (DaaS), entre otras.

Loa modelos de despliegue pueden ser públicos, comunitarios o privados. Teniendo en cuenta la confidencialidad de los datos se pueden combinar distintos modelos Por ejemplo un Cloud privado puede configurar la confidencialidad de los datos en función de las necesidades de los usuarios, pero la escalabilidad de este Cloud puede verse limitada.

Se pueden trasladar el manejo de peticiones de baja prioridad y datos menos relevantes al Cloud público si el privado no tiene disponibilidad. Surge así una nueva alternativa a través de un Cloud híbrido.

El Instituto Nacional de Estándares y Tecnología de USA (NIST) define una infraestructura de Cloud híbrido como: "Una composición de dos o más infraestructuras distintas de Clouds (privado, comunitario o público) que siendo entidades únicas están unidas por tecnología estandarizada o propietaria que permite la portabilidad de datos y aplicaciones" [7].

Este tipo de computación se utiliza cuando la infraestructura interna no puede hacer frente a los desafíos actuales, algunas facilidades son transferidas a un Cloud público (por ejemplo, grandes cantidades de información estadística, que en su forma cruda no tiene un gran valor) permitiendo proporcionar al usuario acceso a los recursos empresariales (para el Cloud privado) a través del Cloud público [8].

Una solución híbrida permite delegar en el Cloud público cierta parte de la información, de forma tal de que no represente una amenaza si ésta es recuperada por usuarios externos y al mismo tiempo permite una alta disponibilidad de los datos almacenados internamente y una disminución en el consumo de recursos [9].

Sin embargo, no es sencillo de lograr una estrategia de gestión eficaz para la implementación de Cloud híbrido, dado que existen muchos problemas a resolver.

A pesar de que ambos Clouds funcionan “emparejados”, pueden existir diferencias de diseño. Cuantos mayores sean estas diferencias, más difícil será gestionar múltiples clouds como una sola entidad.

El Cloud híbrido favorece la redundancia ahorrando costos y mitigando los riesgos de utilizar múltiples centros, pero es necesario resolver la sincronización y el manejo de versiones

Con el proveedor público se realiza un acuerdo de servicio (SLA), que tiene valores pautados Mantener y demostrar el cumplimiento de lo pactado es más difícil en un Cloud híbrido. Hay que asegurar que el proveedor público y privado cumplan lo firmado, se deben buscar los problemas con la integración que podrían interrumpir el servicio y además hay que cerciorarse que los medios de coordinación entre los dos Clouds sean compatibles. Por ejemplo si se trabaja con medios de pagos electrónicos ambos Clouds deben soportan dicho sistema.
Organizaciones con una cartera de aplicaciones grande necesitarán ser capaces de determinar las necesidades de infraestructura de cloud híbrido antes de empezar nuevos desarrollos, o mover las aplicaciones existentes a un entorno de cloud. Diferentes aplicaciones tendrán demandas diferentes en las áreas de cómputo, almacenamiento, seguridad, networking, performance, disponibilidad e identificación [10].
La seguridad resulta un problema importantísimo, no solo de lograr, sino además de garantizar.

Seguridad en modelo Híbrido

La recuperación y la protección de los datos son el asunto más importante en un ambiente basado en Cloud. La seguridad de la base de datos es muy importante para ambas Clouds el local y el público. Existen varios inconvenientes que impactan en la seguridad como: el manejo de recursos y supervisión de los mismos, la falta de reglas estandarizadas para el despliegue y la falta de la normalización.
Reducir el costo de procesamiento es un requerimiento obligatorio de cada organización, pero los datos son siempre la posesión más importante. Ninguna organización puede transferir información a un sistema de terceros si no se construye un puente de confianza [11].
Varias técnicas han sido propuestas por los investigadores para la protección de datos y para lograr el nivel más alto de seguridad, pero existen muchas puntos a resolver para hacerlas más efectivas.
2C híbrido utiliza nuevas APIs, demanda configuraciones complejas, y requiere nuevos conocimientos y habilidades de los administradores de sistema. Estos factores introducen nuevos tipos de amenazas. Esto es así pues los Clouds híbridos son un sistema complejo, sobre los que los administradores tienen una limitada experiencia y esto crea riesgo. Los controles de seguridad tales como la autenticación, la autorización y la gestión de identidad, se deberán trabajar tanto en el sector privado como en el público, integrando estos protocolos de seguridad, ya sea replicando los controles en los dos Clouds y manteniendo los datos de seguridad sincronizados, o utilizando un servicio de gestión de identidad para ambos Clouds.
Para realizar un estudio profundo se deben clasificar los aspectos de seguridad para el 2C híbrido, es por ello que se sugieren 4 categorías: infraestructura, aplicación y plataforma, administración y adherencia o acuerdo. Esta clasificación considera los riegos y otros factores [12].
Varios modelos de DaaS (base de datos como un servicio) proveen el proceso de migración de datos. Los datos pueden migrar de un Cloud a otro, propio o externo. Pero el desafío es realizar la migración con todas las garantías de seguridad como integridad de los datos, confidencialidad, seguridad, portabilidad, privacidad, la exactitud de datos, etc.
Los modelos de seguridad que se aplican surgen de la evolución de la computación y las amenazas que registran los proveedores de servicios y consumidores. Los modelos propuestos son: ITU Security model, The Cloud Multiply Tenancy Model of NIST, Cloud Cube

Model, Sood's Combined Approach y CCMDSM [13].
Los riegos que surgen con 2C se pueden clasificar en áreas críticas que son: seguridad de la información, gestión de terceras partes, administración y control, leyes y regulaciones, recuperación ante desastres y continuidad del negocio, portabilidad e interoperabilidad y riesgos de virtualización [14].
Por lo descripto anteriormente, una visión integral de la seguridad incluye además la recuperación ante desastres, problemas crecientes de migración de datos, lo que teniendo en cuenta la complejidad del modelo híbrido, no se resuelve solamente con algoritmos criptográficos y normas administrativas.

Líneas de Investigación, Desarrollo e Innovación

2C involucra una gran variedad de de tecnologías, además el modelo de despliegue híbrido incluye al modelo público y al privado. Esto determina que los investigadores del grupo tengan que resolver múltiples problemas.
La complejidad del enfoque híbrido radica en la forma de planificar la asignación de procesos y datos entre ambas infraestructuras, gestión de seguridad y otros aspectos, que deben ser solucionados para obtener un balanceo de carga óptimo.
En ambientes académicos existen pocos proyectos sobre Cloud híbridos y la cantidad de publicaciones son escasas.
El grupo de investigación está trabajando en variados aspectos del modelo híbrido y en esta línea de investigación se debe realizar el estudio y análisis de la interoperabilidad y compatibilidad de las distintas estrategias de seguridad para cloud público y privado.

Problemas a resolver en un futuro

La arquitectura de seguridad debe estar asociada a tareas de administración de los recursos como son: gestión de configuración y control de cambios. Por otro lado se deben abordar temáticas vinculadas a la gestión de fallos y gestión de réplicas, extensibilidad, que impactan en la seguridad, siendo la mayoría de éstos son desafíos previstos para futuros proyectos.

Resultados y Objetivos

Resultados Obtenidos

Un proyecto sobre 2C híbrido se está desarrollando desde 2014, a partir del mismo se ha iniciado esta línea de investigación. El grupo ha realizado publicaciones en el área durante el último año: seis (6) trabajos de investigación en diferentes Congresos y Jornadas: dos trabajos en el Workshop de Investigadores en Ciencias de la Computación 2014, dos (2) trabajos en el Congreso Argentino de Ciencias de la Computación 2014, dos (2) trabajos en el CoNaIISI , además se realizaron tres (3) publicaciones en revistas científicas.
Se obtuvo una beca investigación y también se han aprobados cuatro tesinas de grado sobre 2C, Gestión de red para 2C y Mobile 2C.

Objetivos

El objetivo del grupo de investigación es realizar el estudio de los distintos protocolos y estándares para construir una arquitectura de seguridad para 2C híbrido utilizando herramientas libres.

Formación de Recursos Humanos

El equipo de trabajo está compuesto por los seis (6 docentes-investigadores que figuran en este trabajo, 4 alumnos, egresados y un becario de investigación.

Durante 2014 se aprobaron cuatro (4) tesinas de grado. Además se están realizando dos (2) tesinas de licenciatura una sobre Mobile Cloud Computing y otra sobre SOA aplicada a 2C. Se espera realizar también un trabajo de especialización sobre hybrid 2C y dos (2) tesis de maestría una sobre Metodologías de desarrollo aplicadas a SaaS y otra sobre bases de datos NoSQL y además aumentar el número de publicaciones. Por otro lado también se prevé la divulgación de varios temas investigados por medio de cursos de postgrado y actualización o publicaciones de divulgación.

Referencias

[1] D. Zissis, D. Lekkas, "Addressing cloud computing security issues", Future Generation Computer Systems, 28, 583–592, 2012

[2] Rodríguez, Valenzuela, Murazzo, Chávez, Martín, Villafañe, González. Cloud Computing con herramientas libres para evaluación de modelos de despliegue híbrido. WICC Abril 2014. Ushuaia. Tierra del Fuego.

[3] Rodríguez, Murazzo, Chávez, Valenzuela, Martín, Villafañe. Key aspects for the development of applications for Mobile Cloud Computing. Journal of Computer Science & Technology. Vol. 13 - No. 3 – Dec. 2013. Special Issue on "I JCC 2013".

[4] Rodríguez, Murazzo, Villafañe, Valenzuela, Martin, Chávez. Una propuesta para la incorporación de Cloud Computing en la currícula de Grado. Revista Iberoamericana de Tecnología en Educación y Educación en Tecnología (TE&ET). UNLP. La Plata. 2014 vol. n°12. p 37– 43.

[5] Weiss, Computing in the clouds. netWorker Vol 11, Issue 4, page. 16-25. Dec 2007.

[6] S. Rao, N. Rao, Kumari. Cloud Computing: An Overview. Journal of Theoretical and Applied Information Technology. Vol 9 N1. 2009.

[7] NIST Special Publication 800-145. The NIST Definition of Cloud Computing. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[8] Parthipan, Sriprasadh, Maheshkumar. Secure Information Transaction In Hybrid Cloud Computing. Information Communication and Embedded Systems (ICICES). 2013.

[9] Hernández Ramírez. Sistema de almacenamiento de archivos con tolerancia a fallos utilizando Cloud Híbrido. Tesis de Maestría en Computación. Victoria, Tamaulipas, México.2011.

[10] Patel M., Patel R., Chaube A.. Hybrid Cloud Computing: Data Sharing & Security Issues. International Journal of Research (IJR) Vol-2, Issue-1 January 2015 ISSN 2348-6848.

[11] M. Yousaf Saeed, A.Tahir, S. Mughal, M.Khan. Insight into Security Challenges for Cloud Databases and Data Protection Techniques for Building Trust in Cloud Computing. Journal of Basic and Applied Scientific Research. Ag. 2013.

[12] Sharma O., Das P., Kumar Chawda R.. Hybrid Cloud Computing with Security Aspect. International Journal of Innovations & Advancement in Computer Science. IJIACS. Vol. 4, Issue 1. Jan 2015.

[13] Shah N., Chauhan S. Survey Paper on Security Issues While Data Migration in Cloud Computing. 2014 IJIRT. Vol., Issue 7. ISSN: 2349-6002.

[14] Carroll, M., A. van de Merwe, and P. Kotze. 2011, "Secure Cloud Computing: Benefits, Risks and Controls", In Proceedings of the Information Security. South Africa, pp. 1–9.